H GLOSSARY OF ACRONYMS AND TERMS

ADP – Automated Data Processing.

Algorithm – A computational procedure used for performing a set of tasks such as an encryption process, a digital signature process, or a cardholder verification.

Anti-tearing – The process or processes that prevent data loss when a smart card is withdrawn from the contracts during a data operation.

Application Program Interface (API) – A formal specification of a collection of procedures and functions available to a client application programmer. These specifications describe the available commands, the arguments (or parameters) that must be provided when calling the command, and the types of return values when the command execution is completed.

Attribute Authority (AA) – An entity responsible for issuing and verifying the validity of an attribute certificate.

Attribute Certificate – A message, similar to a digital certificate, which is intended to convey information about the subject. The attribute certificate is linked to a specific public key certificate. Thus, the attribute certificate conveys a set of attributes along with a public key certificate identifier or entity name.

Authorization – The process of determining what types of activities or access are permitted for a given physical or logical resource. Once the identity of the user has been authenticated, they may be authorized to have access to a specific location, system, or service.

Automated Response Unit (ARU) – A designated system for answering telephone calls and providing information to callers via recorded messages, or transferring calls to a customer service center (CSC). An automated telephone answering system can provide voice answers to questions using data from the WIC information system. For example, it can be used to remind clients of appointments, respond to client inquiries, and record problem inquiries. The technology is easily adaptable to multi-language use.

Bar Code – The set of vertical bars of irregular widths representing coded information placed on consumer products and other items (such as identification cards) that may require this type of identification. The vertical lines of varying widths, or other more complex encoding patterns enable fast, automated identification of or explanation about an item such as food instruments, vouchers, clients, and foods. Bar codes are not new technologies. However, the type, complexity, security, and data density of bar coding encryption patterns has increased significantly in the last few years. The ease of use, speed, and costs of equipment for handling such codes have also improved dramatically. There is a widespread and commonly used infrastructure that supports common use of this form of data encoding and exchange. While its use within WIC is still largely limited to identification numbers on ID cards and UPC's on foods, there is the potential for WIC information systems to take advantage of the increasing potential of this technology.

Binding – An affirmation by a Certificate Authority/Attribute Authority (or its acting Registration Authority) of the relationship between a named entity and its public key or biometric template.

Biometric Template – Refers to a stored record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on an integrated circuit chip card. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template.

Biometrics – An automatic identification process for identity verification of individuals based on unique behavioral or physiological characteristics. These are unique things that we do or unique physical characteristics that we have. Behavioral biometrics include voice, signature, and keyboard typing technique. Physical biometrics include fingerprint, hand geometry, facial recognition, and iris and retinal scan.

Bridge Certificate Authority – An entity that links two or more Certification Authorities who do not have a cross-certification agreement in place. The Bridge Certificate Authority allows CAs to validate each other's certificates.

CDC – Centers for Disease Control and Prevention.

CPA – Competent Professional Authority.

CPU – Central Processing Unit.

CSFP – Commodities Supplemental Food Program.

CASE - Computer Aided Software Engineering. CASE tools allow organizations to develop system functional requirements, entity relationship diagrams, data warehouses, and other data models.

Caseload – The number of WIC participants that can be supported by a given food grant amount. Generally, caseload management processing includes the translation of food grant dollars into caseload estimates, the collection and storage of information on caseload allocations to local agencies, and the tracking of actual participation against assigned caseloads.

Centralized Processing – A data processing architecture in which the mechanism for processing data (i.e., the Central Processing Unit (CPU)) is located in a single, central environment such as a data center. Typically, various terminals or PCs are used to access the processing capability maintained in the central location. A mainframe kept in a centralized data center is an example of a centralized processing architecture. Usually, the mainframe has terminals/PC's in separate geographic locations connected to the mainframe in the central location. The geographically dispersed terminals/PCs collect data/transactions locally but send these transactions over a network to be processed by the CPU in the mainframe. No processing is performed locally at the site of the terminal/PC.

Certificate Authority (CA) – The Certificate Authority is a component of the Public Key Infrastructure. The CA is responsible for issuing and verifying digital certificates. Digital certificates may contain the public key or information pertinent to the public key.

Certificate Arbitrator Module (CAM) – A system that interfaces with agency applications that receives a request for the status of a certificate, passes the certificate validation request to the appropriate CA, receives the certificate validation request response, returned from the CA, and reports the response to the requesting agency application.

Certificate Policy – A document that sets forth the rules established by the policy issuing entity governing the issuance, maintenance, use, reliance upon, and revocation of digital certificates.

Certificate Repository – A database of certificates and other PKI relevant information available on-line.

Certificate Revocation List (CRL) – A periodically issued list, digitally signed by a CA, of identified certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked certificates' serial numbers, and the specific times and reasons for suspension and revocation.

Certification –The process of determining the eligibility of an applicant for receipt of WIC benefits. The applicant must be categorically eligible, income (or adjunctively eligible) eligible, and at nutritional risk to be certified.

Certification Practice Statement (CPS) – A document that states the practices that a Certificate Authority employs in issuing certificates.

Civil Money Penalties (CMPs) – State agencies often assess claims for misuse of program funds against vendors. Monetary payments received from vendors because of assessed sanctions by the vendor management or program integrity staff may be used for food or NSA expenditures.

Compliance Monitoring – The investigation of WIC vendors to ensure that they adhere to WIC regulations. Compliance monitoring may include compliance buys, routine monitoring visits, and vendor record reviews.

Compromise – A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.

Computer-Based Training (CBT) – A training program individual users can use on their workstation to provide remedial or advanced instruction of functions. It provides a grading of the training session.

Conversions – If approved by FNS, use of food funds for NSA costs. A State agency may also use NSA funds for food funds at any time.

Cryptography – The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

Customer Service Center (CSC) – A customer service unit staffed with operators or Customer Service Representatives (CSR).

Customer Service Representatives (CSR) – Customer Service Representatives are responsible for taking telephone calls and providing information and services to clients as needed.

DTR – Registered Dietetic Technician.

Data Integrity – A condition in which data has not been altered or destroyed in an unauthorized manner.

Data Warehouse – A data warehouse is a collection of data in support of management's decision-making process that is *subject-oriented; integrated; time-variant; and non-volatile.* A data warehouse is generally focused on a business concept (for example, claims statements) rather than a business process (for example, paying claims), and contains all the relevant information on the concept gathered from multiple processing systems. This information is collected and represented at consistent periods of time, and is not changing rapidly (except that new data is added). A data warehouse is a copy of transaction data specifically structured for query and analysis.

Digital Certificate – A portable block of data, in a standardized format, which at least identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certificate authority issuing it.

Digital Signature – A unique electronic signature that accompanies documents and messages. The digital signature serves two primary functions: verifies the authenticity of the party sending the message, and verifies that the content of the message has not been altered.

Digitized Signature – A written signature that has been read by a computer scanner and converted into digital data. It is a capability for recording signatures on an electronic device in a digital format. The most common publicly visible use at present is in capturing signature images for credit card purchases in retail stores. More expensive units can be used as one means of electronic identification.

Distributed Processing – A data processing architecture in which the mechanism for processing data (i.e., the CPU) is located at dispersed geographic locations. Both the data collection and the data processing are performed locally. Data for a single system may be processed at many locations. Some systems allow data to be processed locally, but uploaded to a central storage capacity.

Distinguished Name – A set of data that identifies a real-world entity, such as a person in a computer-based context.

Dual Participation – The term used to describe a person who receives nutritional food benefits from more than one source (e.g., multiple clinics).

EDC – Estimated Date of Confinement.

EPSDT – Early and Periodic Screening, Diagnosis, and Treatment Program.

Electronic Benefits Transfer (EBT) – The use of electronic mechanism to transfer value from a program to a benefit recipient (EBT functions are described in FRED-E).

Electronic Cash Register (ECR) System (also referred to as an Electronic Payment System (EPS) – An in-store automated system that electronically scans items for purchase, obtains the UPC code and price for the item, adds the item to the cash register receipt, and totals the entire purchase to arrive at a purchase total.

Electronic Purse – A mechanism that allows end users to pay electronically for goods and services. The function of the electronic purse is to maintain a pool of value that is decremented as transactions are performed.

Electronic Service Delivery (ESD) – Use of a unique client identifier and advanced electronic technology to provide integrate and efficient client centric service delivery (ESD functions are described in FRED-E).

Encryption – Refers to the process of translating data into a cipher, a more secure form of data. Encrypted data is less likely to be intercepted and accessed by unauthorized persons. This mechanism is particularly important in executing sensitive transactions.

Enrollee – An applicant who has been certified as eligible for WIC benefits, but to whom food benefits have not yet been issued.

FNS – USDA Food and Nutrition Service.

FRED – Functional Requirements Document.

FSP – Food Stamp Program.

FTE – Full Time Equivalent.

False Acceptance Rate (FAR) – Refers to the rate at which an unauthorized individual is accepted by the system as a valid user.

False Rejection Rate (FRR) – Refers to the rate at which an individual authorized to use the system is rejected as an invalid user.

Food Instrument (FI) – The printed paper vouchers or food checks that document the specified WIC foods and the amounts of these foods for a specified period of time that have been prescribed for a WIC participant and that can be redeemed at an authorized WIC vendor.

Food Package – The set of foods recommended for specific categories of WIC participants and/or risk factors. Food packages may be tailored for individual participants because of special nutritional needs, incomplete benefit periods, etc.

Food Prescription – The specific set of foods prescribed by a nutritionist for an individual WIC participant for a specified period of time.

Generate Standard Reports – Standard reports provide pre-defined data sets in a consistent format and can be requested through a report menu. These recurring reports can be displayed on the screen, printed in hard copy, or saved to a file for later printing or import into another software product. To allow for some limited customization of standard reports, the system may allow users to enter data selection or sort parameters to limit the scope of data included in the report or method of presenting the data.

Geographic Information System (GIS) – A system that processes geographic information such as mapping of geographic points or areas or using mathematical algorithms for measuring distance.

Graphical User Interface (GUI) – A user interface to a computer that is graphics-based, rather than textual or command-based.

Hashing – A software process which computes a value (hashword) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.

Identification Authentication – The process of determining the identity of a user that is attempting to access a physical location or computer resource. Authentication can occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, or other techniques.

I/C – Infant or Child.

Information System (IS) – The information system is the software application that automates WIC processing.

International Standards Organization (ISO) – A worldwide organization dedicated to fostering the development of systems standards. National standards organizations from 100 different countries are members of the ISO, including the United States (American National Standards Institute – ANSI). Member organizations participate in the development of ISO standards.

Interoperability – Refers to a system or a product that is capable of operating with another system or product directly, (i.e. without any additional effort from the user). Interoperability can be achieved through mutual conformance to a set of common standards and specifications. Interoperability may also be achieved through the use of a “service broker” able to convert one interface into another interface directly.

Key – A value that particularizes the use of a cryptographic system.

Key Management – The process and means by which keys are generated, stored, protected, transferred, loaded, used, revoked, published, and destroyed.

Key Pair – The key pair consists of a private key and its matching public key.

Kiosk – A public access terminal, located at various locations within the community, at which users may access one or more computer applications. The kiosk may provide access to an application housed in a central data processing facility, based on the Internet, or resident locally in the central processing unit of the kiosk. A kiosk typically has an enclosure with light box, a touch screen display, a printer, a PIN pad, card reader (if used for a card application), a CPU or PC, and a power supply. Both freestanding and desktop versions may be used. Often touch-screen technology that prompts the client to select a function by touching an option displayed on the screen is used. To be effective, kiosk applications must be straightforward, easily learned and understood without training, and usable by most or all of the intended audience with little or no training.

LMP – Last Menstrual Period.

Lightweight Directory Access Protocol (LDAP) – LDAP is an emerging software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

Local Area Network (LAN) – The connectivity of computing hardware (workstations, printers, scanners, etc.) generally within a building for the purpose of allowing the sharing of computing resources. Connectivity can be wired/cabled or wireless (using radio frequencies or infra-red transmissions).

Maintain Data Warehouse – The most complex level of reporting requires synthesis of data from multiple systems over extended periods of time. The requestor is often attempting sophisticated research to identify trends in data over historical periods. For this type of multifaceted data analysis, a data warehouse may be the most effective tool. A data warehouse is a collection of data in support of management's decision-making process that is subject-oriented; integrated; time-variant; and non-volatile. The data warehouse is focused on a business concept (for example, claims statements) rather than a business process (for example, paying claims), and contains all the relevant information on the concept gathered from multiple processing systems. This information is collected and represented at consistent periods of time, and is not changing rapidly. Thus, a data warehouse generally includes data extracted periodically from multiple legacy systems, combined in a single, separate reporting database.

The fundamental basis of any useful data warehouse is that it retains similar data from many sources, over a long period of time, in a single format that is effective when used in their intended manner. However, they can be burdensome and inefficient if misused as a general purpose tool.

Building the data warehouse requires a set of tools for describing the logical and physical design of the data sources and their destinations in the data warehouse. Operational data must pass through a cleansing and transformation stage before being placed into the data warehouse in order to conform to the definitions laid out during the design stage. End user tools, including desktop productivity products, specialized analysis products and custom programs are used to gain access to the information in the data warehouse. Ideally, user access is through a directory facility that enables the user to search for appropriate and relevant data to resolve business questions, and provides a layer of security between the users and the back-end systems. The structure of the database for the data warehouse is quite different from the structure for a transaction management system. The data warehouse utilizes On-line Analytical Processing (OLAP) technologies that allow the user to construct queries "on-the-fly" that build upon preceding queries and are modified in real time depending on the results of the previous analysis.

MDS – Minimum Data Set.

Magnetic Ink Character Recognition (MICR) – Ink that has a magnetic content used on documents that can be scanned into a reader to recognize characters. For example, used on personal checks, food instrument checks/vouchers.

Mean Time Between Failures (MTBF) – The estimated length of time that a system is available and operational between failures.

Mean Time To Repair (MTTR) – The estimated length of time needed to bring a system back up and make it fully operational following a system failure.

NSA Grant – Nutrition Services and Administration Grant.

Non-repudiation – Refers to the determination that data was sent by one party and received by another party, and can be verified by the inclusion of information about the origin or delivery of the data. Non-repudiation protects both the sender and the recipient of data from false claims that the data was either not sent, or not received.

NWA – National WIC Association (formerly NAWD, or National Association of WIC Directors).

OST – Out of State Transfer.

Open Database Connectivity (ODBC) – Refers to an open or standard application programming interface (API) used to access a database. A database that is ODBC-compliant facilitates the importing, exporting and converting of files from external databases.

Open Systems Environment – A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. An open platform is composed of hardware and software components that adhere to common standards and are non-proprietary such that multiple vendors can supply these components interchangeably. In an open platform, components from multiple vendors using different technological approaches may be assembled and interoperability across products can be ensured. The objective of an open platform is to achieve vendor independence and allow easy transition to emerging technologies.

PC Report – Federal Participant Characteristics Report that is prepared every two years from a Minimum and Supplemental data set transmitted by the State agency to FNS. The data set contains a census of specific participant data items for the month of April.

PP – Postpartum Woman.

Palm-Held Computers – Small computers whose size corresponds to a hand that that can used where it is inconvenient to use or carry a laptop computer. For WIC, it can be used in a clinic where it is inconvenient to carry a laptop computer, or recording food prices at a vendor location. Can transfer data to a larger computer via wired or infra-red transmission.

Participant – A client of WIC who has been certified and to whom food benefits have been issued (this includes breastfed infants).

Participant Care Plan – An individualized plan set up for each WIC participant that tracks health and nutrition goals, suggested nutrition education, and desired outcomes from the WIC program for individual participants over time.

Password – Confidential authentication information, usually composed of a string of characters used to provide access to a computer resource.

Peer Group – A vendor peer group is a subset of approved vendors of similar size, or location, client population.

Personal Data Assistants (PDA) (Also referred to as Palm-Held Computers) – Another small computational device for handling information.

PLU – Price Look Up code.

Point of Sale (POS) – Generally refers to a site where purchases are made. For the purposes of this document, POS refers to a site where purchases may be made electronically through an electronic cash register or card acceptance device.

Primary Account Number (PAN) – A unique identifying number used to reference a financial account.

Private Key – A mathematical key (kept secret by the holder) used to create digital signatures, and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Proxy – A person designated by a WIC participant to access food benefits (e.g., a pregnant woman's husband may be designated as a proxy so he can shop for her).

Public (Asymmetric) Key Cryptography – A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public Key Infrastructure (PKI) – The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Further, a communications infrastructure that allows users to exchange money and data over the Internet in a secure environment. There are four basic components to the PKI: the certificate authority (CA) responsible for issuing and verifying digital certificates, the registration authority (RA) which provides verification to the CA prior to issuance of digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Included also in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

Public Key – A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

RD – Registered Dietician.

RDA – Recommended Dietary Allowance.

RN – Registered Nurse.

Radio Frequency Identification (RFID) – Refers to an access control system that features a tag embedded with both a circuit and an antenna. As the antenna enters the electronic field of the reader, it generates energy for the circuit, and transmits the identification number in the tag to the reader.

Rebate – A discounted amount of the purchase price of a WIC item that is returned to the State Agency on each item for which there is a rebate contract in place with a given manufacturer. The

State Agency bills the manufacturer either for the estimated or actual amount of rebated products purchased (usually monthly), depending on the capabilities of the WIC information system.

Registration Authority (RA) – The Registration Authority is a component of the Public Key Infrastructure. The RA acts as a gatekeeper by providing verification to the Certificate Authority before granting a request for a digital certificate.

Relying Party – A recipient who acts in reliance on a certificate and digital signature.

Renewal – The process of obtaining a new certificate of the same class and type for the same subject once an existing certificate has expired.

Revocation – The process of permanently ending the operational period of a certificate from a specified time forward. Generally, revocation is performed when a private key has been compromised.

Root – The CA that issues the first certificate in a certification chain. The root's public key must be known in advance by a certificate user in order to validate a certificate chain.

S&B – Salaries and Benefits.

SAM – State Agency Model.

SOAP – Subjective, Objective Assessment Plan.

SNP – Special Nutrition Program.

Secret (Symmetric) Key Cryptography – A cryptographic system that uses the same key, known as a "secret key algorithm" to encipher and decipher messages. This is contrasted with asymmetric key cryptography, which uses a secure public/private key pair.

Secure Access Module (SAM) – A software module contained in a card access device that allows the card and terminal to mutually authenticate each other.

Security – Features and procedures used to reduce the possibility of fraudulent use, asset compromise, smart card counterfeiting, or other subversion.

Security Policy – A document that articulates requirements and good practices regarding the protections maintained by a trustworthy system.

Speaker Identity Verification (SIV) – The key feature of voice recognition software that extracts and compares unique features of a speech sample with a known sample, and accepts or rejects access based on this comparison.

Spendback – A financial management strategy that supports prior year over expenditures with the use of current year funds.

Spendforward – A financial management strategy that supports current year expenditures by using prior year unspent funds.

Storage – An electronic and/or mechanical-magnetic device that holds information for subsequent use or retrieval.

Subscriber – A person who is the subject of, has been issued a certificate, and is capable of using, and authorized to use, the private key that corresponds to the public key listed in the certificate.

TANF – Temporary Assistance to Needy Families.

Tampering – Refers to any unauthorized alteration or modification of a card.

TIP Report – The Integrity Profile, an annual report about WIC vendors required by FNS that includes vendor characteristics, training, compliance activities, and sanctions.

Token – A hardware security token containing a user's private key(s), public key certificate, and optionally other certificates.

UPC – Universal Product Code.

Verification of Certification (VOC) – A paper or electronic document that carries a participant's certification data to be used to very that the participant has already been certified by another local agency when the participant moves to a new location.

Vendor – A grocery retailer authorized by the WIC program to sell WIC foods and redeem WIC food benefits.

Vendor Sanction – An action taken against a vendor who is not in compliance with WIC regulations.

Verification of Certification (VOC) – A paper or electronic card provided to a participant who is moving to a new location. The card provides proof of certification so that the new local agency can immediately serve the participant until the end of his/her certification period.

VPN – Virtual Private Network (or Private Virtual Network) VPNs use advanced encryption to allow entities to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets.

WIC – Special Supplemental Nutrition Program for Women, Infants and Children

Web-Based Data Collection – A computer application that presents a data entry form via the Internet. A Web Browser is used to present the Web page containing the data collection form to the user who can then enter data directly into the form displayed on the Web page. The data collected through this form can be reformatted or translated and transmitted via a network to other data processing systems.

Wide Area Network (WAN) – Connectivity typically of smaller networks over a large, geographical area.

Wireless Network – normally used in place of a cabled/wired local area network. Can be used in portable/mobile situations. Radio or light devices are used instead of wires or cables to conduct transmissions of data, programs, etc.